



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/578,633	05/25/2000	Steven Branigan	1-1-7	5753
22046	7590	09/21/2005	EXAMINER	
LUCENT TECHNOLOGIES INC. DOCKET ADMINISTRATOR 101 CRAWFORDS CORNER ROAD - ROOM 3J-219 HOLMDEL, NJ 07733			ZIA, SYED	
			ART UNIT	PAPER NUMBER
			2131	

DATE MAILED: 09/21/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

<b>Office Action Summary</b>	<b>Application No.</b> 09/578,633	<b>Applicant(s)</b> BRANIGAN ET AL.	
	<b>Examiner</b> Syed Zia	<b>Art Unit</b> 2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

#### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

#### Status

- 1) ☒ Responsive to communication(s) filed on 17 June 2005.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

#### Disposition of Claims

- 4) ☒ Claim(s) 1-3,6-12,14-24,26 and 27 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-3,6-12,14-24,26 and 27 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

#### Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

#### Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

#### Attachment(s)

- |  |   |
|--|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892)   | 4) <input type="checkbox"/> Interview Summary (PTO-413)<br>Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)                                   | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152)             |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)<br>Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____  |

## **DETAILED ACTION**

### ***Continued Examination Under 37 CFR 1.114***

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on June 10, 2005 has been entered.

### ***Response to Amendment***

This office action is in response to amendment filed on June 10, 2005. Original application contained Claims 1-27. Applicant previously amended Claims 1-2, 6-11, 14,15, 6, 18-24, and 26-27. Applicant previously cancelled 4-5, 13, and 25. Applicant argument filed on November 26, 2004 have been entered and made of record. Therefore, presently pending claims are 1-3, 6-12, 14-24, and 26-27.

### ***Response to Arguments***

Applicant's arguments filed June 10, 2005 have been fully considered but they are not persuasive because of the following reasons:

Art Unit: 2131

Regarding Claim rejection 35 U.S.C. 112, Examiner finds the claims, which this limitation indefinite because it is unclear as to what Applicant regards as the security characteristic. The language of the claims, claim 1 in particular, states the security characteristic is determined as a function of a response by the probed host but there is not a clear indication as to whether the security characteristic is an entity or quantity. The security characteristic could be interpreted as a packet, a probe echo, a firewall, or even some indication of connection. The claim language, which states the security characteristic is a measure of connectivity, further adds to the ambiguity of the claim.

Regarding Claims 1, 10, 16, 21, and 24 applicants argued that in the cited prior art (CPA) [Shostack (U.S. Patent No. 6,298,445) "*second module (and, for that matter fourth module) is not performing and does not anticipate, teach or suggest Applicants' claimed invention. In particular, the fact that Shostack's fourth module essentially implements --on a remote basis--the functionality of the second module does not teach or suggest Applicants' claimed invention. Applicants' claimed invention is directed at discovering connectivity of, or between, a host machine (or host machines) as function of response (or absence thereof) to specifically configured probe packet*".

And also argued that "*claimed invention directed to utilizing a probe packet to determine a connectivity measure between two communication networks (where the packet includes a source address which is associated with a second communications network*".

This is not found persuasive. The system of cited prior art teaches and describes a computer security system modules for accessing security vulnerabilities on networks such as internet, intranet, extranet, etc. where modules (74,76,78) are used for accessing a data base and

Art Unit: 2131

the security vulnerability of a computer network, and modules (88,90) are used for accessing security vulnerability of a remote computer connected to the network and for receiving and updating to data base respectively.

Cited prior art teaches a fourth module of this system which allows a remote computer to first connect to a network service and like the second network module, interrogates the service. Examiner references column 12, lines 41-57 as the teaching of what module two does. Specifically module two carries out the network scan and generates a map of the network and scans the ports for known security vulnerabilities. Therefore module four does this from a remote location. The remote location would then have a source address associated with a second communications network. An address that is different from the first communications network.

Cited prior art also teaches a sixth module which is a communication module that allows an integrated security system to communicate with a similar system over a computer network. In line 27, the module invokes remote systems. In line 34, Shostack teaches that this sixth checks the integrity of the service connection. This teaching is another example of communication between networks to perform the security functions of cited prior art invention.

The examiner has pointed to two separate teachings where cited prior art teaches or suggests utilizing a probe packet to determine a connectivity measure between the two communication networks where the packet includes a source address which is associated with a second communication network.

Therefore, the examiner asserts that user obtains instant access to the latest security vulnerabilities and employs immediate remedial action before a security breach occurs, and

Art Unit: 2131

automatic enhancements are made for the database of security vulnerabilities, thus providing a security solution to potential weak computer or computer network. Thus, the system of prior art provides robustness of security measures and ensuring that network security features are universally configured throughout a commemorations network.

Applicants clearly have failed to explicitly identify specific claim limitations, which would define a patentable distinction over prior arts. The examiner is not trying to interpret the invention but is merely trying to interpret the claim language in its broadest and reasonable meaning. The examiner will not interpret to read narrowly the claim language to read exactly from the specification, but will interpret the claim language in the broadest reasonable interpretation in view of the specification. Therefore, the examiner asserts that the system of cited prior arts does teach or suggest the subject matter broadly recited in independent Claim 1, 10, 16,21,and 24 and in subsequent dependent Claims. Accordingly, rejections for claims 1-3, 6-12, 14-24, and 26-27 are respectfully maintained.

### ***Claim Objections***

Applicant amended the claim to overcome the objection. Therefore, previous objection has been withdrawn.

***Claim Rejections - 35 USC § 112***

The following is a quotation of the first paragraph of 35 U.S.C. 112:

The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

1. Claim 1, 10, 16, 21, and 24 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention. The subject matters “security characteristic” and “an indication of connectivity” is not enabled in the specification, and it is not clear what is being measured regarding security characteristic of the probed network when measuring characteristic is only an indication of connectivity. Is measure of indication of connectivity pertains to available bandwidth, traffic load or the integrity of the network? .
2. Claim 7, 20, and 23 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention. The limitation “different security levels” is not defined and described in the specification. Does “different security levels” means access authentication for users, or security policy implemented on the network in general and on firewall in particular?

***Claim Rejections - 35 USC § 102***

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

1. Claims 1-3, 6-12, 14-24, and 26-27 are rejected under 35 U.S.C. 102(e) as being anticipated by Shostack et al (USP 6,298,445).

As per claims 1 and 24, Shostack et al teach a communications network security method for ascertaining the integrity of a first communication network and identifying potential security risks across a perimeter of the first communications network, the method comprising:

identifying a plurality of routes that define the first communications network  
(column 12, lines 41-57),

identifying a plurality of hosts as a function of the plurality of routes (column 12, lines 41-57),

performing a census of the communications network as a function of the plurality of hosts to determine a topology of the communications network (column 12, lines 41-57);

probing at least one first host of the plurality hosts by transmitting a packet to the first host, the first host being selected from the census results and the packet having at least a



Art Unit: 2131

source address of a second host which is associated with a second communications network determined as a function of the topology, wherein the source address is selected independent of any request from the second host to the first host; (column 12, lines 41-57), and

determining a security characteristic of the probed first host as a function of a response by the probed first host in receiving the packet, the security characteristic being a measure of connectivity between the first communications network and the second communications network the measure of connectivity being an indication of connectivity between first communication network and the second communication network (column 12, lines 41-57 and column 13, lines 1-5).

As per claims 2, Shostack et al teach the source address of the second is a return IP address (column 1, lines 64-65 and column 3, lines 1-4).

As per claims 3 and 26, Shostack et al teach the response of the probed first host to the receipt of the packet includes transmitting a second packet, the second packet being derived using at least a portion of information from the received packet (column 5, lines 20-35).

As per claim 6, Shostack et al teach the determining the security characteristic operation further comprises:

monitoring the probed first host to determine the response, and if the response

Art Unit: 2131

includes a transmission of a second packet from the probed first host to the second host at the return IP address, generating a security alert message identifying the probed first host as a security risk (column 7, lines 5-19).

As per claim 7, Shostack et al teach the first and second communications network have different security levels (column 13, lines 1-5).

As per claim 8, Shostack et al teach the transmitted packet is a TCP packet (column 5, lines 24-45).

As per claim 9, Shostack et al teach the second packet is a UDP packet or an ICMP packet (column 5, lines 24-45).

As per claim 10, Shostack et al teach a method for analyzing network security across a perimeter of a first communications network utilizing a security host, the method comprising: receiving a census of the first communication network (column 12, lines 41 -57); transmitting, from the security host a packet associated with a host of a second communications network to a particular one host of the plurality of hosts internal to the communications network, the internal host being selected from the census, and the packet having an IP source address associated with the host of the second communications network, wherein the IP source address is selected independent of any request from the host of the second communications network to the internal host of the first communications network (column 13, lines 1-6); and

Art Unit: 2131

determining a security characteristic of the particular one internal host as a function of a response by the internal host to the receipt of the packet, the security characteristic being a measure of connectivity between the first communications network and the second communications network (column 12, lines 41-57 and column 13, lines 1-5).

As per claim 11, Shostack et al teach the determining the security characteristic operation further comprises: monitoring the probed host to determine the response, and if the response includes a transmission of a second packet, utilizing the IP source address, from the internal host to the host of the second communication network, generating a security alert message identifying the probed host as a security risk (column 7, lines 5-19, and column 13, lines 1-5).

As per claim 12, Shostack et al teach the second packet is derived using at least a portion of information from the transmitted packet (column 5, lines 24-45).

As per claim 15, Shostack et al teach the security characteristic includes an indication that the probed host is outside any security measures provide by a firewall associated with the communications network (column 9, lines 10-18).

As per claim 16, Shostack et al teach a communications system for ascertaining the integrity of a first communication network and identifying potential security risks across a perimeter of the first communication network, the communication system comprising:

a first plurality of computers associated with the first communications network; a second plurality of computers associated with a second communications network, and a security host computer which determines a security characteristic of a first computer from the first plurality of computers, the security characteristic being a measure of connectivity between the first communications network and the second communications network (column 13, lines 1-5) performs a census of the communications network as a function of the first plurality of computers, and probes the first computer by transmitting a packet to the first computer, the first computer being selected from the census results and the packet being generated as a function of an IP source address associated with a second computer of the second plurality of computers, wherein said IP source address is selected independent of any request from the second computer to the first computer, and an IP address associated with the first computer, and determining a security level associated with the first computer as a function of a response of the first computer to receiving the packet the measure of connectivity being an indication of connectivity between the first communications network and the second communication network (column 12, lines 41-57, column 1, lines 64-65, and column 3, lines 1-4).

As per claim 17, Shostack et al teach the security host computer is associated with the first communications network (column 4, lines 33-34).

As per claim 18, Shostack et al teach the response of the probed host to the receipt of the packet includes transmitting a second packet, the second packet being derived using at least a portion of information from the received packet (column 5, lines

Art Unit: 2131

20-35).

As per claim 19, Shostack et al teach the determining the security characteristic operation further comprises:

monitoring the probed host to determine the response, and if the response includes a transmission of a second packet from the probed host, generating a security alert message identifying the probed host as a security risk (column 7, lines 5-19).

As per claims 20 and 27, Shostack et al teach the first communications network is an intranet and the second communications network is an Internet (column 4, lines 14-21) and the two network communications have different security levels (column 13, lines 1-5).

As per claim 21, Shostack et al teach a security host computer for ascertaining the integrity of a first communication network and identifying potential security risks across a perimeter of the first communication network, the security host computer comprising:

means for performing a census of the communications network and determining a topology of a first communications network, the topology being defined by at least One Computer (Column 12, lines 41 -57);

means for probing the at least one computer by transmitting a packet to the computer, the computer being selected from the census results and the packet being generated as a function of (i) the topology, (ii) an IP source address associated with a particular host computer associated

Art Unit: 2131

with a second communications network, wherein the IP source address is selected independent of any request from the second computer to the first computer and (iii) an IP address associated with the computer, the second communications network being separate from the first communications network (column 12, lines 41-57); and

a monitor for determining a security level of the computer as a function of a response by the computer to the receipt of the packet (column 12, lines 41-57) the security characteristic being a measure of connectivity between the first communications network and the second communications network (column 13, lines 1-5).

As per claim 22, Shostack et al teach the measure of connectivity is determined by monitoring the computer the response, and if the response includes a transmission of a second packet, utilizing the IP source address, from the computer, a security alert message identifying the computer as a security risk is generated (column 7, lines 5-19).

As per claim 23, Shostack et al teach the security level is determined with respect to a firewall located between the first communications network and the second communications network (column 4, lines 14-21).

***Claim Rejections - 35 USC § 103***

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claim 14 is rejected under 35 U.S.C. 103(a) as being unpatentable over Shostack et al in view of Sitaraman et al (USP 6,212,561 ).

As per claim 14, Shostack et al teach that all known security attacks are stored in a database so they can be tested against the host of an intranet (column 2, lines 48-60).

Shostack et al's teachings disclose a method that protects an intranet from the Internet.

Sitaraman et al teach that one security risk to an intranet is a multi-homed host inside of an intranet (column 3, lines 40-49). Therefore, it would be advantageous for a system that secures intranets to check the intranet for hosts that are multi-homed.

In view of this, it would have been obvious to one of ordinary skill in the art at the time the invention was made to employ the teaching of Sitaraman et al with the system of Shostack et al because it would allow the system to guard against users which try to connect to the Internet while still being connected to the secure intranet. One skilled in the art would have been motivated to generate the claimed invention with a reasonable expectation of success.

Art Unit: 2131

***Conclusion***

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Syed Zia whose telephone number is 571-272-3798. The examiner can normally be reached on 9:00 to 5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).



SZ

September 5, 2005